CLAIMS

What is claimed is:

1. A monitoring device (1) for a data processing system (2) in a network comprising network connections (4), for protecting data storage and/or data transmission means of the data processing system against unauthorized access, the data processing system comprising a disabling circuit (6) for interfaces (8, 10, 12, 14),

characterized in

that only a single data storage means (9) is connected to a bootable interface (8) of the data processing system (2) as a mainboot device that can boot freely,

that other bootable interfaces (10, 12, 14) are disabled at first, and

that at least one of the interfaces (10, 12, 14) disabled by the disabling circuit (6) is enabled from a data processing point (16) located at a distance in the network via the network connection (4) after authorization of an authorized person at the data processing point (16).

2. The monitoring device of claim 1, characterized in that the disabling circuit (6) disables the bootable interfaces (10, 12, 14) via a CMOS.

3. The monitoring device of one of claims 1 or 2, characterized in that the disabling circuit (6) is integrated on the motherboard.

4. The monitoring device of one of claims 1 or 2, characterized in that the disabling circuit (6) is arranged on a separate card with a separate interface, preferably a PCI card.

5. The monitoring device of one of claims 1 to 4, characterized in that the disabling circuit (6) includes a microcontroller.

6. The monitoring device of one of claims 1 to 5, characterized in that the disabling circuit (6) is controlled by the data processing point (16) through a receiving line (22) of the network connection (4).

7. The monitoring device of one of claims 1 to 6, characterized in that the disabling circuit (6) comprises a reset line (24), preferably a power reset.

8. The monitoring device of one of claims 1 to 7, characterized in that an alarm circuit (28, 30, 32, 34) is connected to at least one bootable interface (8, 10, 12, 14), said alarm circuit preferably being connected to the network connection (4) and being adapted to transmit an alarm signal via the network connection and, further, preferably being connected to a free mass port of the interface (8, 10, 12, 14).

9. The monitoring device of one of claims 1 to 8, characterized in that a housing of the data processing system (2) is provided with an alarm circuit (36), preferably a key switch, which is preferably connected to the network connection (4) and is adapted to transmit an alarm signal via the network connection (4).

10. The monitoring device of one of claims 1 to 9, characterized in that at least one plug-in connection for a keyboard and/or a universal serial port of the data processing system (2) is provided with an alarm circuit (38), preferably a socket switch, which is preferably connected to the network connection (4) and is adapted to transmit an alarm signal via the network connection (4).

11. The monitoring device of one of claims 1 to 10, characterized in that the network connection (4) is protected against unauthorized access, such as pulling off one or a plurality of terminal pins, for example, by means of an alarm circuit.

12. The monitoring device of one of claims 8 to 11, characterized in that one or a plurality of the alarm circuits (28, 30, 32, 34, 36, 38) is connected to a transmission/receiving line strand (26a) of the network connection (4), preferably to individual lines (4a-d).

13. The monitoring device of claim 12, characterized in that the alarm circuits (28, 30, 32, 34, 36, 38) are connected in parallel through resistors (40) and are combined to one line (42).

14. The monitoring device of claim 13, characterized in that the combined alarm circuits (28, 30, 32, 34, 36, 38) are connected to two lines of the network connection (4) through a star wiring and two coils (44), that an alarm detection means (46) is connected to the two lines of the network connection (4), remote from the data processing system (2), through a star wiring and two coils (48), and that an alarm transmission path is established over a phantom line.

15. The monitoring device of one of claims 8 to 12, characterized in that at least two capacitors (50) are provided in individual lines (4a-d) of the network connection (4), respectively.

16. The monitoring device of claim 15, characterized in that the alarm circuits (28, 30, 32, 34, 36, 38) are connected to the individual lines (4a-d) of the network connection (4) by a star wiring between the capacitors (50).

17. The monitoring device of one of claims 15 or 16, characterized in that an alarm detection means (46) is connected, remote from the data processing system (2), to the individual lines (4a-d) of the network connection (4) by a star wiring between the capacitors (50).

18. The monitoring device of claim 14 or 17, characterized in that the alarm detection is effected by monitoring a rest current applied to the alarm circuits (28, 30, 32, 34, 36, 38) via the network connection.

19. The monitoring circuit of claim 18, characterized in that the rest current is generated dynamically by a random-check generator (52), that the rest current is supplied to the alarm circuits (28, 30, 32, 34, 36, 38) on the one hand and to a parallel reference circuit (54) on the other hand, and that the rest currents applied in parallel are monitored at a comparator point (56).

20. The monitoring device of one of claims 1 to 12, characterized in that one or a plurality of the alarm circuits (28, 30, 32, 34, 36, 38) is connected to a separate line strand (26b) of the network connection (4), preferably to individual lines (4e-h), respectively.

21. The monitoring device of claim 20, characterized in that an alarm detection means (46) is connected, remote from the data processing system (2), to the individual lines (4e-h) of the separate line strand (26b) of the network connection (4).

22. The monitoring device of claim 21, characterized in that the alarm detection is effected by monitoring a rest current applied to the alarm circuits (28, 30, 32, 34, 36, 38) via the network connection (4).

23. The monitoring device of one of claims 8 to 22, characterized in that an alarm triggered causes a device, e.g. a bolt gun, to mechanically destroy at least one access-protected data carrier of the data processing system (2).

24. The monitoring device of one of claims 8 to 23, characterized in that a circuit for triggering the alarm manually, e.g. with a manual switch, is provided at at least one of the alarm circuits (28, 30, 32, 34, 36, 38).

25. A method for monitoring a data processing system (2) in a network comprising network connections (4), for protecting data storage and/or data transmission means of the data processing system (2) against unauthorized access,

characterized in

that, upon booting, only a single data storage means can be accessed at a bootable interface (8) of the data processing system (2),

that other bootable interfaces (10, 12, 14) are disabled at first, and

that the disabled interfaces (10, 12, 14) are enabled from a data processing point (16) located at a distance in the network via the network connection (4) after authorization of an authorized person at the data processing point (16).

26. The method of claim 25, characterized in that the disabling of the interfaces (10, 12, 14) is controlled by the data processing point (16) via a receiving line of the network connection (4) and a disabling circuit (6).

27. The method of one of claims 25 or 26, characterized in that the disabling of the bootable interfaces (10, 12, 14) is restored to the disabled state after the data processing system (2) has been switched off and/or after a user has logged off at the data processing system (2).

28. The method of one of claims 25 to 27, characterized in that an alarm is triggered at a remote alarm detection means (46) by removal of a data storage means and/or of a data transmission means of the data processing system (2), as well as by opening a housing of the data processing system (2).

29. The method of claim 28, characterized in that the alarm can be triggered manually, e.g. by means of a switch.

30. The method of one of claims 28 or 29, characterized in that a mechanical destruction of at least one access-protected data carrier of the data processing system (2) is caused by an alarm triggered.